

# EXHIBIT A

THE HONORABLE JOHN C. COUGHENOUR

UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
AT SEATTLE

REBECCA COUSINEAU, on her own  
behalf and on behalf of all others similarly  
situated,

Plaintiff,

v.

MICROSOFT CORPORATION,  
Defendant.

CASE NO. C11-1438-JCC

ORDER REGARDING  
DEFENDANT'S MOTION TO  
DISMISS

This matter comes before the Court on Defendant's motion to dismiss (Dkt. No. 22), Plaintiff's response (Dkt. No. 25), and Defendant's reply (Dkt. No. 27). Having thoroughly considered the parties' briefing and the relevant record, the Court finds oral argument unnecessary and hereby DENIES in part and GRANTS in part the motion for the reasons explained herein.

**I. BACKGROUND**

This case involves an alleged invasion of privacy resulting in the transmission of sensitive information on the location and movement of smart phone users. Rebecca Cousineau brought this class action suit against Microsoft Corporation seeking to represent "[a]ll persons in the United States that, prior to August 31, 2011, denied their Windows Phone 7 camera application access to their location information, and unwittingly had their geolocation data

transmitted to Microsoft’s servers.” (Am. Compl. ¶ 34 (Dkt. No. 19 at 8).) Microsoft moved to dismiss the Complaint pursuant to Rule 12(b)(1), lack of subject matter jurisdiction, and Rule 12(b)(6), failure to state a claim upon which relief can be granted.

The following facts are undisputed except as otherwise indicated. Cousineau owns a smart phone operating Microsoft Windows Phone OS 7 software (OS 7). OS 7 supports “geolocation services”—a system that approximates users’ location and enables users to locate friends and businesses, tag a photograph with location data, or find a missing phone. To operate geolocation services, OS 7 collects and stores six different types of information: a unique phone identifier,<sup>1</sup> a unique application identifier, the current date and time, the approximate latitude and longitude of the phone, the locations of the nearest cellular towers, and unique wireless router MAC addresses. (Research Doc. 2–6 (Dkt. No. 19, ex. A); (Microsoft Let’r (Dkt. No. 1, ex. A at 3–5).) When users enable geolocation services, the phone transmits geolocation information to Microsoft’s servers and to the application requesting the information. (Dkt. No. 1, ex. A at 5.) Microsoft stores users’ geolocation information on servers containing its master database, the contents of which, according to Cousineau, were published online by Microsoft. (Dkt. No. 19 at 5 ¶¶ 18–19.) OS 7 also stores geolocation information on the phones themselves to help users find a lost phone, request location information, and improve Microsoft’s database where GPS, WiFi access point, and cell tower data is lacking. (Dkt. 1, ex. A at 7–8.)

At issue in this case is Microsoft’s design of the on-off switch controlling geolocation services on smart phones’ camera application. The camera prompts users to choose whether to allow access to their geolocation information with the following message:

[a]llow the camera to use your location? Sharing this information will add a location tag to your pictures so you can see where your pictures were taken. This

---

<sup>1</sup> With respect to unique phone identifiers, Microsoft has stated that it “recently discontinued its storage and use of device identifiers” and that the next update of its software “will no longer send device identifiers to the location service and new phones arriving this fall will not send device identifiers to the location service.” (Dkt. No. 1, ex. A at 6.)

information also helps provide you with improved location services. We won't use the information to identify or contact you.

(Dkt. 19 at 3 ¶ 4.) Cousineau claims that even when she denied access by clicking "cancel," her geolocation information was still transmitted to Microsoft. She supports her claim by presenting individual HTTPS packets transmitted from the phone to Microsoft, which appear to reveal that Microsoft received the location data after she denied access (as well as before the privacy prompt appeared). (Dkt. No. 19, ex. A at 3.) Microsoft counters that in order to disable location services properly, users needed to disable it in two places—on the phone's main settings menu, *and* when prompted by the individual application (here, the camera application).

In April 2011, the House Committee on Energy and Commerce inquired into Microsoft's collection of users' location data and its ability to track users. In its response on May 9, 2011, Microsoft emphasized its respect for users' privacy preferences, stating "[c]ollection is always with the express consent of the user." (Dkt. No. 1, ex. A at 2, 6, 10.) Microsoft asserted on the one hand that, "information we collect and store helps us determine where those landmarks are, not where device users are located," and in the very next sentence that "we've recently taken specific steps to eliminate the use and storage of unique device identifiers by our location service . . . . Without a unique identifier . . . we cannot track an individual device." (*Id.* at 3.) Later in the letter, Microsoft further explained that "[w]hile collecting device identifiers can help assemble and refine a database of available WiFi access points and cell towers more quickly and effectively than without them, these identifiers have diminishing value over time," and that it discontinued the collection of device identifiers in the subsequent version of the software. (*Id.* at 6.) After the filing of this Complaint and the submission of Microsoft's letter to Congress, Microsoft acknowledged in an online press release that it had discovered "unintended behavior" of the sort Cousineau now complains. (Dkt. No. 19 at 3 ¶ 7 FN 1 (citing Microsoft, *Location and My Privacy FAQ*, Windows Phone Privacy, <http://www.microsoft.com/windowsphone/en-US/howto/wp7/web/location-and-my-privacy.aspx> (last updated Dec. 2011)).) Even when users

1 had disabled location services on their phones' camera, the phone continued to transmit their  
2 location information. *Id.*

3 Cousineau alleges that Microsoft deceived users by purposefully designing a defect in OS  
4 7's privacy control on the camera application, while maintaining publicly that it respected their  
5 privacy. She states: "Microsoft made very specific representations to U.S. Congress members  
6 about the very functionality of its Windows Phone OS 7 that the [Microsoft] now claims is  
7 flawed." (*Id.* at 7 ¶ 29.) Furthermore, "[t]he idea that, during the programming process, these  
8 software engineers simply 'overlooked' the fact that their own code was designed to ignore  
9 users' refusal to consent to be tracked is untenable" because "Microsoft is one of the largest and  
10 most renowned software developers in the world, with a highly sophisticated staff of engineers."  
11 (*Id.* at ¶ 28.) Cousineau doubts the truthfulness of Microsoft's statements to Congress because  
12 she believes that Microsoft would have investigated the problem thoroughly before representing  
13 the company's absolute respect for users' privacy. (*Id.* at ¶ 29.) In addition, Cousineau submits  
14 HTTPS packets that purport to show that Microsoft continued to collect unique device identifiers  
15 as late as August 27, 2011, even though it represented to Congress that it had "recently  
16 discontinued its storage and use of device identifiers." (Dkt. No. 1, ex. A at 6.)

17 Finally, Cousineau alleges that Microsoft used the unauthorized data it collected to  
18 improve geolocation services and to facilitate the development of targeted advertisements to  
19 smart phone users based on their location. (Dkt. No. 19 at 4-5 ¶ 14-15.) She claims that  
20 Microsoft's conduct is motivated by the projected 2.5 billion dollar mobile advertisement  
21 industry. (*Id.* at 4 ¶¶ 13-14.)

## 22 **II. DISCUSSION**

23 Cousineau claims that Microsoft's conduct violated the following four statutes: the  
24 Stored Communications Act, 18 U.S.C. §§ 2701, *et seq.*, the Wiretap Act, 18 U.S.C. §§ 2510, *et*  
25 *seq.*, the Washington Privacy Act, WASH. REV. CODE § 9.73, *et seq.*, the Washington Consumer  
26

1 Protection Act, WASH. REV. CODE § 19.86, *et seq.* In addition, she alleges that Microsoft was  
2 unjustly enriched at her expense. Microsoft now moves to dismiss.

3 The Court first considers Microsoft's motion to dismiss the Complaint for lack of subject  
4 matter jurisdiction on standing grounds, and second, its motion to dismiss for failure to state a  
5 claim upon which relief may be granted. Fed. R. Civ. P. 12(b)(1), (12)(b)(6).

6 **A. Whether Cousineau has Standing to Bring Her Claims**

7 Cousineau has standing to bring this action if she has asserted (1) an injury in fact that is  
8 concrete and particularized, (2) a causal connection between the injury and the conduct  
9 complained of, and (3) that the injury is redressable by a favorable decision. *See Lujan v.*  
10 *Defenders of Wildlife*, 504 U.S. 555, 560 (1992). Solely at issue here is Microsoft's contention  
11 that its mere receipt of Cousineau's location information did not injure her sufficiently to confer  
12 standing. (Dkt. No. 22 at 9, 15.)

13 The Court focuses its review on Cousineau's standing to bring claims under the Stored  
14 Communications Act ("SCA"). At this point, the Court need not reach her standing to bring  
15 claims under the Wiretap Act, Washington Consumer Protection Act, Washington Privacy Act or  
16 unjust enrichment doctrine because, as discussed later on, she has not stated a claim entitling her  
17 to relief with respect to those causes of action.

18 **1. Cousineau's Standing to Bring a Claim Under the Stored**  
19 **Communications Act**

20 The primary intent of the Stored Communications Act is to protect the privacy of  
21 individuals' personal information by prohibiting the government and private parties from  
22 accessing that information. *See* 18 U.S.C. §§ 2701 (a)(1), (a)(2). More specifically, the Ninth  
23 Circuit has explained that the SCA:

24 reflects Congress's judgment that users have a legitimate interest in the  
25 confidentiality of communications in electronic storage at a communications  
26 facility. Just as trespass protects those who rent space from a commercial storage  
facility to hold sensitive documents, *cf. Prosser and Keeton on the Law of Torts* §  
13, at 78 (W. Page Keeton ed., 5th ed. 1984), the Act protects users whose

1 electronic communications are in electronic storage with an ISP or other  
2 electronic communications facility.

3 *Theofel v. Farey-Jones*, 359 F.3d 1066, 1072–73 (9th Cir. 2004).<sup>2</sup>

4 It is well established that “[t]he actual or threatened injury required by Art[icle] III may  
5 exist solely by virtue of statutes creating legal rights, the invasion of which creates standing.”

6 *Warth v. Seldin*, 422 U.S. 490, 500 (1975) (internal citation and quotation marks omitted).

7 Cousineau asserts her SCA claim pursuant to a private right of action provided by the Act under  
8 18 U.S.C. § 2707. Even with this private right of action, however, “Art. III’s requirement  
9 remains: the plaintiff still must allege a distinct and palpable injury to himself, even if it is an  
10 injury shared by a large class of other possible litigants.” *Warth*, 422 U.S. at 501. For this reason,  
11 the Court considers whether Cousineau’s alleged injury is concrete and particularized for the  
12 purpose of Article III standing.

13 Cousineau alleges several facts that demonstrate that her alleged privacy injury is both  
14 concrete and particularized. Not only does Cousineau own a mobile device running OS 7, but the  
15 facts she alleges demonstrate, with significant detail, how the defect in the camera application  
16 led to the loss of her location data. First, Cousineau submits a photograph of the privacy  
17 statement she read prior to disabling geolocation services. Second, the HTTPS packets she  
18 submits purport to show that she “disabled” geolocation services on her phone’s camera. Third,  
19 the packets appear to reveal—packet-by-packet—each type of information that the phone  
20 continued to transmit to Microsoft.

---

21  
22 <sup>2</sup> Microsoft argues that the main purpose of the SCA is to punish and deter computer  
23 hackers. While Microsoft correctly cites to *Konop v. Hawaiian Airlines, Inc.*, in which the Ninth  
24 Circuit stated that computer hacking “was a major concern of Congress in enacting the  
25 Electronic Communications Privacy Act and the Stored Communications Act,” 302 F.3d 868,  
26 889 (9th Cir. 2002), neither that case nor the cases to which it cites provide a single reference to  
statutory history which reflects that purpose. The statute has already been applied in contexts  
outside of computer hacking, and nothing prevents this Court from considering other, very  
similar harms for which this statute may provide a remedy.

1 Cousineau's submissions in support of her claimed injury are substantially more concrete  
2 and particularized than what plaintiffs have offered in recent consumer privacy cases involving  
3 new technology. *See, e.g., Low v. LinkedIn Corp.*, No. 11-CV-01468-LHK, 2011 WL 5509848,  
4 at \*3 (N.D. Cal. Nov. 11, 2011) (dismissing a case for lack of standing where plaintiff failed to  
5 articulate what information defendant allegedly disclosed to third parties, how that information  
6 was transferred, and that his identity was linked to his sensitive internet browsing history); *In re*  
7 *iPhone Application Litig.*, No. 11-MD-02250-LHK, 2011 WL 4403963, at \*4 (N.D. Cal. Sept.  
8 20, 2011) (finding that plaintiffs asserting privacy violations against mobile device makers  
9 lacked standing where they failed to identify what devices they used, what applications they  
10 downloaded, or whether any defendants actually accessed plaintiffs' personal information); *La*  
11 *Court v. Specific Media, Inc.*, No. SACV 10-1256-GW, 2011 WL 2473399, at \*3-4 (C.D. Cal.  
12 Apr. 28, 2011) (finding that plaintiffs' alleged injury was not particularized where plaintiffs had  
13 failed to allege that the defendant online advertisement company had actually tracked their  
14 internet activity, or that they were affected by the defendant's conduct).

15 Cousineau's allegation that Microsoft intentionally deceived her intensifies the severity  
16 of her alleged injury. First, she alleges that her camera's privacy prompt misled her to think she  
17 controlled Microsoft's access to her data. Second, she emphasizes that Microsoft misrepresented  
18 its privacy practices to Congress. As previously noted, in its letter to Congress, Microsoft  
19 explicitly stated that it only collects users' location information with their consent. (Dkt. No. 1,  
20 ex. A at 2, 6, 10.) Further, Microsoft emphasized that it "recognizes that consumers should have  
21 control over the location information they share and that the information should be narrowly  
22 tailored to support specific experiences on Windows Phone 7 devices." (*Id.* at 3.) Microsoft's  
23 press release disclosing its discovery of "unintended behavior," however, appears to contradict  
24 the representations it made to Congress only a few months prior. (Dkt. No. 19 at 3 ¶ 7 FN 1  
25 (citing Microsoft, *supra* at 3).) On these facts, it is plausible that Microsoft gained access to  
26 users' data by subterfuge, a fact that is indicative of tortious intent under Washington law. *See*

1 *Mark v. Seattle Times*, 635 P.2d 1081, 1094 (Wash. 1981) (citing approvingly to *Dietemann v.*  
2 *Time, Inc.*, 449 F.2d 245, 249 (9th Cir. 1971), in which the court found news reporters liable for  
3 intruding on plaintiff's privacy when they gained entrance into his home by subterfuge and  
4 recorded him with hidden electronic devices); *cf. Peters v. Vinatieri*, 9 P.3d 909, 918 (Wash. Ct.  
5 App. 2000) (finding no privacy invasion where video was filmed from a publicly open place and  
6 involved no subterfuge); *Mark v. King Broadcasting Co.*, 618 P.2d 512, 519 (Wash. Ct. App.  
7 1980) (same).

8 Of particular concern is Microsoft's alleged collection of unique phone identifiers  
9 because of their potential to enable Microsoft or another company to link users' personal  
10 information with their current physical location. *U.S. Dep't of State v. Ray*, 502 U.S. 164, 176  
11 (1991) ("Although disclosure of [individuals'] personal information constitutes only a *de*  
12 *minimis* invasion of privacy when the identities of the [individuals] are unknown, the invasion of  
13 privacy becomes significant when the personal information is linked to particular  
14 [individuals]."). Microsoft's purported collection of sensitive data to which it was expressly  
15 denied access distinguishes this case from recent cases involving companies' placement of  
16 "cookies" on browsers to collect information regarding users' internet activity. For example, in  
17 *In re DoubleClick Inc. Privacy Litigation*, the court highlighted the fact that plaintiff internet  
18 users had voluntarily and purposefully requested information from, and entered personal  
19 information into, the websites they visited. 154 F. Supp. 2d 497, 511 (S.D.N.Y. 2001); *see also*  
20 *Low*, 2011 WL 5509848 (finding plaintiffs lacked standing to sue social networking website for  
21 disclosing information to third parties when plaintiffs voluntarily posted that information on the  
22 website). In contrast, Cousineau expressly signaled her intent to protect her privacy by clicking  
23 "no" when asked if she wanted to allow the camera application to use her location.<sup>3</sup>

24  
25 <sup>3</sup> The fact that Cousineau apparently failed to disable location services on the master  
26 settings of her phone does not vitiate her alleged privacy injury. This is so because the presence  
of the on-off switch created a reasonable expectation of privacy. *See United States v. Katz*, 389  
U.S. 347, 352 (holding, in a constitutional context, that affirmative acts of concealment create an

1 On the whole, the Court is satisfied that Cousineau has met the concrete and  
2 particularized standard for injury in fact that the Constitution demands.

3 **B. Whether Cousineau has Adequately Pled Her Five Claims**

4 In addition to seeking dismissal on the basis that Cousineau lacks standing, Microsoft  
5 seeks dismissal on the basis that Cousineau failed to allege sufficient facts to support the  
6 elements of each of her five claims. A motion to dismiss pursuant to Rule 12(b)(6) “tests the  
7 legal sufficiency of a claim.” *Navarro v. Block*, 250 F.3d 729, 732 (9th Cir. 2011). To survive a  
8 12(b)(6) motion, “a complaint must contain sufficient factual matter, accepted as true, to ‘state a  
9 claim to relief that is plausible on its face.’” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting  
10 *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). In reviewing a motion to dismiss, the  
11 Court draws all reasonable inferences from those facts in favor of the plaintiff. *Al-Kidd v.*  
12 *Ashcroft*, 580 F.3d 949, 956 (9th Cir. 2009) *rev’d on other grounds*, 131 S. Ct. 2074 (2011).  
13 Although Rule 12(b)(6) neither requires courts to evaluate the merits of a plaintiff’s claim, nor  
14 requires the plaintiff to plead “detailed factual allegations,” the allegations in the complaint must  
15 cross “the line between possibility and plausibility of entitlement to relief.” *Iqbal*, 556 U.S. at  
16 678 (quoting *Twombly*, 550 U.S. at 555–57). “A claim has facial plausibility when the plaintiff  
17 pleads factual content that allows the court to draw the reasonable inference that the defendant is  
18 liable for the misconduct alleged.” *Id.* (quoting *Twombly*, 550 U.S. at 556).

19 In this case, there are no short cuts to fully understanding the technical capability and the  
20 legal implications of Microsoft’s alleged invasion of Cousineau’s privacy. If Cousineau has  
21 alleged sufficient facts to satisfy the plausibility standard, the Court would be remiss in  
22 dismissing the case without further factual development.

23  
24  
25 expectation of privacy because “[o]ne who . . . shuts the [phone booth door] behind him, and  
26 pays . . . to place a call is surely entitled to assume the words he utters into the mouthpiece will  
not be broadcast to the world”).

1                   **1. Cousineau’s Stored Communications Act Claim**

2           Cousineau contends that Microsoft programmed OS 7 to store location information  
3 without users’ consent and that in doing so, it violated the Stored Communications Act. (Dkt.  
4 No. 19 at 11 ¶¶ 46–47.) The SCA provides a private right of action where an individual or entity  
5 does one of the following:

- 6                   (1) intentionally accesses without authorization a facility through which an electronic  
7                   communication service is provided; or  
8                   (2) intentionally exceeds an authorization to access that facility;  
9                   and thereby obtains, alters or prevents authorized access to a wire or electronic  
10                  communication while it is in electronic storage in such system . . . .  
11                  18 U.S.C. § 2701(a).

12           Microsoft takes issue with three main aspects of Cousineau’s SCA claim. First, Microsoft  
13 claims that Cousineau does not allege that Microsoft accessed a “facility.” Second, Microsoft  
14 asserts that Cousineau fails to allege access to any “electronic communications” held in  
15 “electronic storage.” Third, Microsoft claims that the SCA’s provider-consent provision  
16 authorizes its action. The Court considers each objection in turn.

17                   **a. Whether Cousineau’s Mobile Device is a Facility**

18           The Court first considers whether Cousineau’s mobile device is a “facility” within the  
19 meaning of the SCA. Congress did not define the term “facility,” and Microsoft maintains that  
20 Congress could not have intended it to encompass a mobile device. (Def.’s Mot. to Dismiss 18  
21 (Dkt. No. 22).) The Court disagrees. Congress chose a broad term—facility—where it intended  
22 the statute to cover a particular function, such as internet access, as opposed to a particular piece  
23 of equipment providing that access, such as a router, laptop or smart phone. As technology  
24 evolves, identifying a smart phone as a facility through which an ECS is provided is not as  
25 “strained” as it once may have seemed. *See Chance v. Avenue A, Inc.*, 165 F. Supp. 2d 1153,  
26 1161 (W.D.Wash. 2001) (leaving open the possibility that personal computing devices are  
“facilities” under the SCA); *United States v. Park*, No. CR 05-375 SI, 2007 WL 1521573 at \*8

(N.D. Cal. May 23, 2007) (explaining that the line between cell phones and computers has blurred because “[i]ndividuals can store highly personal information on their cell phones, and can record their most private thoughts and conversations on their cell phones through email and text, voice and instant message”). While earlier stages of technological development may have required large facilities for data storage, the draw of mobile devices is that their smaller storage space enables communication and information access regardless of the user’s location. Viewing a mobile device as a facility also comports with the common definition of “facility.” Webster’s Dictionary defines “facility” as “something that promotes the ease of any action, operation, transaction or course of conduct.” Webster’s Third New International Dictionary 812 (3d ed. 2002). A chief purpose of smart phones is to “promote the ease” of actions such as navigating from place to place, sharing information with others, and capturing images. On the whole, the Court is satisfied that a mobile device can be a facility for the purposes of the SCA.

**b. Whether Cousineau has Plausibly Alleged that Microsoft Accessed “Electronic Communications” Held in “Electronic Storage”**

The Court next considers whether Cousineau has plausibly alleged access to “electronic communications” held in “electronic storage.” The SCA defines “electronic communication service” as “any service which provides to users thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. § 2510(15). Cousineau contends that Microsoft is not an ECS provider because its services are more akin to “traditional products and services [sold] over the internet.” (Pl.’s Resp. 17:20–25 (Dkt. 25).) To the contrary, Microsoft’s geolocation services are not bought and sold like books sold on Amazon or hotels booked through Expedia. Because OS 7 provides users the “ability to send or receive electronic communications,” the Court finds that Microsoft is an ECS provider for the purposes of the SCA.

Next, the SCA prohibits only unauthorized access to a facility through which ECS are *provided*. 18 U.S.C. § 2701(a)(1). Microsoft argues that § 2701 does not apply because “Microsoft *provides* location services through its own facilities, such as servers and transmitters; Cousineau makes *use* of the services through her phone, running Windows Phone 7.” (Dkt. 22 at

1 18:12–14.) The language Congress chose, however, does not require only one point of ECS  
2 provision as Microsoft suggests. None of the facts Microsoft presents preclude the Court from  
3 finding that geolocation services are both provided by Microsoft in its installation of OS 7 on a  
4 phone *and* supported by its servers. While the parties would benefit from discovery on this issue,  
5 at this stage, it is plausible that a device on which OS 7 operates is a facility through which ECS  
6 is provided.

7 **c. Whether Microsoft’s Actions Were “Authorized”**

8 The third major issue raised by Microsoft is whether its alleged conduct in accessing data  
9 was “authorized” for the purpose of the SCA. As Microsoft recognizes, even if Cousineau’s  
10 mobile device is a facility through which Microsoft provides ECS under § 2701(a), Microsoft  
11 may still be immune from liability if one of the SCA’s authorization exceptions applies. The  
12 Court now considers this issue.

13 Section 2701(c) sets out several exceptions to the § 2701(a) prohibitions. Pertinent here is  
14 the “ECS provider-consent” exception. The “provider-consent” exception, set out at §  
15 2701(c)(1), states that the prohibitions of § 2701(a) do not apply to conduct authorized “by the  
16 person or entity providing a wire or electronic communications service.”

17 Microsoft argues that even if the facts Cousineau alleges meet the terms of § 2701(a), its  
18 conduct remains exempt from liability under the ECS provider-consent exception. The Court,  
19 however, cannot agree. As Cousineau vigorously argues, it would be entirely unjust to conclude  
20 that Microsoft could enable users to ostensibly control their privacy settings—thereby  
21 encouraging them to believe that their privacy is secure—and then hide behind the provider-  
22 consent provision when it fails to respect those privacy settings. In other words, Microsoft is not  
23 entitled to assure its customers that they have control over the privacy of their information while  
24 simultaneously retaining full authorization to access any user data it wishes. The Court therefore  
25 finds that the provider-consent exception does not apply here because Microsoft voluntarily  
26

1 limited its own authorization to access consumer data in designing and marketing a phone with  
2 user-controlled privacy settings.

3 The Court's conclusion that the provider-consent exception does not apply is also  
4 supported by the legislative history of the SCA, which indicates that the exception was intended  
5 to ensure that ECS providers were able to access certain private information where necessary to  
6 maintain service. *See* S. Rep. No. 541, 99<sup>th</sup> Cong., 2nd Sess. Reprinted in, 1986 U.S.C.C.A.N.  
7 3555, 3574 ("The provider of electronic communications services may have to monitor a stream  
8 of transmissions in order to properly route, terminate, and otherwise manage the individual  
9 messages they contain."). There is no question here that Microsoft did not *need* access to  
10 Cousineau's information for purposes of maintaining its system.

11 In sum, the Court finds that Cousineau has stated a plausible claim that Microsoft  
12 violated the SCA.

## 13 **2. Cousineau's Wiretap Act Claim**

14 In her second claim, Cousineau charges that Microsoft violated 18 U.S.C. § 2511(1)(a)  
15 and § 2511(1)(d) when it intentionally intercepted and used the contents of her geolocation  
16 information after it was transmitted without her consent. (Dkt. No. 19 at 13 ¶ 54–55.) Section  
17 2511(1)(a) of the Wiretap Act supplies a cause of action against any person who "intentionally  
18 intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to  
19 intercept, any wire, oral, or electronic communication." Section 2511(1)(d) provides a cause of  
20 action against any person who "intentionally uses or endeavors to use the contents of any wire,  
21 oral or electronic communication, knowing or having reason to know that the information was  
22 obtained . . . in violation of this subsection." Key to applying the Wiretap Act to the facts of this  
23 case are two definitions the statute provides. First, § 2510(4) defines the term "intercept" to  
24 mean "the aural or other acquisition of the contents of any wire, electronic, or oral  
25 communication through the use of any electronic, mechanical, or other device." Second, §  
26

1 2510(8) defines the term “contents” to include “any information concerning the substance,  
2 purport, or meaning of that communication.”

3 Microsoft challenges Cousineau’s Wiretap Act claims on several grounds; however, its  
4 first ground is determinative. Microsoft argues that the term “contents” does not encompass  
5 geolocation data, and therefore, Cousineau’s claims under both § 2511(1)(a) and § 2511(1)(d)  
6 must fail. The Court agrees.

7 The Court first considers Congress’s construction of its prohibitions under § 2511(1)(a)  
8 and § 2511(1)(d). By its use of the term “intercepts” Congress incorporated the definition of the  
9 term “contents” into the prohibition against intercepting communications under § 2511(1)(a).  
10 Congress also expressly referred to “contents” in its prohibition of the use of unlawfully  
11 intercepted communications under § 2511(1)(d). As Microsoft notes, the Wiretap Act therefore  
12 requires a defendant’s conduct to have touched the “contents” of plaintiff’s wire, oral, or  
13 electronic communication in order to state a claim under *both* § 2511(1)(a) and § 2511(1)(d).  
14 Thus, the Court must consider whether the term “contents” is broad enough to encompass  
15 Cousineau’s geolocation data.

16 Cousineau contends that Congress intended the term “contents” to be interpreted broadly  
17 and that the term logically includes location information. To find that the packets she has  
18 submitted provide information concerning the “substance, purport, or meaning” of a  
19 communication, however, strays too far from even a broad interpretation of the term “contents.”  
20 Nor does Cousineau cite any authority to support this proposition. The conclusion that the term  
21 “contents” does not include location information is consistent with other courts’ recent findings  
22 that cell-site location information (“CSLI”) does not constitute the contents of a communication  
23 under § 2510(8). A close look at the nature of CSLI reveals that it is extremely similar to the  
24 information that was allegedly transferred to Microsoft. One court described CSLI as the cell  
25 phone’s unique identification number which is transmitted to cell towers, and which can “with a  
26 fair degree of precision” approximate the location of the phone based on the location of the

towers. *See In re Application of the United States for an Order Authorizing the Use of Two Pen Register & Trap & Trace Devices*, 632 F. Supp. 2d 202, 205 (E.D.N.Y. 2008). The court in *In re § 2703(d) Order* specifically found that wireless access point MAC addresses, data which Cousineau alleges Microsoft intercepted, are records and not contents under § 2510(8).<sup>4</sup> 787 F. Supp. 2d 430, 436 (E.D. Va. 2011); *see also In re Application of the United States for an Order Directing a Provider of Elec. Comm'n Serv. to Disclose Records to the Gov't*, 620 F.3d 304, 307-08 (3d Cir. 2010) (finding that there is “no dispute that historical CSLI is a record or other information”) (internal quotation marks omitted). For this reason, the court disagrees with Cousineau’s contention that the six types of data she alleges Microsoft unlawfully intercepted “far exceed[] the scope of traditional ‘CLSI’ records.” (Dkt. No. 25 at 21:12–13.)

In conclusion, the threshold requirement that a defendant intercept or use the “contents” of a communication in order to violate § 2511(1)(a) and § 2511(1)(d) of the Wiretap Act forecloses Cousineau from stating a claim for relief under those provisions.

### 3. Cousineau’s Washington Consumer Protection Act Claim

Cousineau makes a compelling argument that Microsoft acted deceptively in causing the Windows Phone 7 to transmit data after users expressly denied it approval to do so. However, her claim under the Washington Consumer Protection Act (“CPA”) must fail because she has not alleged sufficient facts to demonstrate injury to business or property—a crucial element of a CPA claim. To state a claim for relief under the CPA, a plaintiff must establish (1) an unfair or deceptive act or practice (2) occurring in trade or commerce, (3) a public interest impact, (4) injury to the plaintiff’s business or property, and (5) causation. *Hangman Ridge Training Stables, Inc. v. Safeco Title Ins. Co.*, 719 P.2d 531, 533 (Wash. 1986).

Cousineau describes in detail the ways in which Microsoft intentionally designed illusory privacy controls, its motives for doing so, and the resulting imminent threat to many users’

---

<sup>4</sup> Although the courts in these cases were considering CSLI in the context of the SCA, the SCA and Wiretap Act share § 2510(8) for its definition of contents.

1 information. The Court is satisfied that Cousineau has pled sufficient facts to establish the first  
2 three elements of a CPA claim under *Hangman*. Nevertheless, she fails to allege specific facts to  
3 establish the fourth element of her claim—that the phone’s dysfunction caused injury to her  
4 business or property.

5 To establish injury to business or property under the CPA, “[m]onetary damages need not  
6 be proved; unquantifiable damages may suffice.” *Panag v. Farmers Ins. Co. of Wash.*, 204 P.3d  
7 885, 900 (Wash. 2009). But while the “injury involved need not be great, it must be established.”  
8 *Hangman*, 719 P.2d at 539.

9 In support of her CPA claim, Cousineau argues first that Microsoft’s conduct diminished  
10 the value of her phone, and second that the unauthorized transmission of data “to its servers  
11 caused a diminution in users’ data plans.” (Dkt. No. 19 at 16 ¶ 74–75.) Cousineau provides no  
12 support for the assertion that the covert tracking diminished the phone’s market value. However,  
13 the Court does not foreclose the possibility that unauthorized data transmission would be a  
14 cognizable injury to a cell phone user’s personal property where that user purchased a finite  
15 allowance of data.

16 In her Amended Complaint, Cousineau does not allege she paid a wireless carrier for a  
17 finite allowance rather than an unlimited usage plan. Nor does she allege that most members of  
18 the purported class are thought to have finite allowance plans. Even drawing all reasonable  
19 inferences in her favor, the facts Cousineau alleges are too nebulous to demonstrate that  
20 Microsoft’s conduct drained data usage that would have otherwise been available to her.<sup>5</sup>

21 In the absence of more specific facts demonstrating that she or members of the purported  
22 class actually sustained injury, Cousineau’s claim under the CPA must fail.

23  
24  
25 <sup>5</sup> The court disagrees, however, with Microsoft’s urging that Cousineau be required to  
26 show Microsoft’s conduct caused her to exceed her data allowance. (Dkt. No. 22 at 29.) Even a  
*de minimis* depletion of a finite resource one would otherwise have been able to use constitutes  
an injury to personal property regardless of whether or not one is charged an overage penalty.

1                   **4. Cousineau’s Washington Privacy Act Claim**

2           Cousineau claims that Microsoft violated the Washington Privacy Act (“WPA”) when it  
3 intentionally intercepted location data transmitted from her phone without first obtaining her  
4 consent. (Dkt. 19 at 14 ¶¶ 58–61.) In *State v. O’Neill*, the Washington Supreme Court stated that  
5 the purpose of the WPA is “to protect the privacy of individuals by prohibiting public  
6 dissemination . . . of illegally obtained information.” 700 P.2d 711, 725 (Wash. 1985). To this  
7 end, the WPA prohibits individuals or entities from intercepting or recording any,

8           (a) Private communication transmitted by telephone, telegraph, radio, or other device  
9 between two or more individuals . . . by any device . . . without first obtaining the  
consent of all the participants in the communication; [or]

10           (b) Private conversation, by any device . . . without first obtaining the consent of all the  
11 persons engaged in the conversation.

12 RCW § 9.73.030(1). With respect to subsection (a), unlike the federal SCA and Wiretap Act, the  
13 WPA requires a communication between at least two individuals. *See* § 9.73.030(1)(a). As  
14 applied in this case, the term “private communication” raises the following question: if Microsoft  
15 intercepted Cousineau’s communication, as she argues, with whom was Cousineau  
16 communicating? Without an individual on the other end of her communication (other than  
17 Microsoft), the transmission of Cousineau’s data cannot be considered a communication under  
18 the WPA.

19           With respect to subsection (b), expanding the definition of “conversation” to encompass  
20 the transmission of geolocation data would be equally problematic. While the Washington  
21 Supreme Court has not specifically defined the term “private conversation,” it indicated that the  
22 term should be construed within its “ordinary connotation of oral exchange, discourse, or  
23 discussion.” *State v. Smith*, 540 P.2d 424, 428 (Wash. 1975) (finding that a tape recording did  
24 not intercept a private conversation under § 9.73.030(1) because the sounds of gunfire, running,  
25 and shouting were not an oral exchange, discourse, or discussion). Construing the word  
26 “conversation” to include the transmission of geolocation data would stray too far from the

1 term's ordinary meaning. Cousineau's claim fails because the unintended transmission of her  
2 geolocation data constitutes neither a communication nor a conversation under § 9.73.070.  
3 Therefore, she fails to state a claim for relief under the WPA.

#### 4 **5. Cousineau's Unjust Enrichment Claim**

5 Cousineau claims that Microsoft was unjustly enriched in two ways: first, when she  
6 overpaid for her defective phone, and second, when Microsoft unlawfully took her data to  
7 improve its systems and develop its mobile marketing campaign. (Dkt. No. 19 at 17 ¶ 81; Dkt.  
8 No. 25 at 28–29.) In *Young v. Young*, the Washington Supreme Court determined that “[u]njust  
9 enrichment is a method of recovery for the value of [a] benefit retained, absent any contractual  
10 relationship, because notions of fairness and justice require it.” 191 P.3d 1258, 1262 (Wash.  
11 2008). To state a claim for unjust enrichment, Cousineau must plead sufficient facts under each  
12 of the following elements: (1) that Microsoft received a benefit, (2) at Cousineau's expense, and  
13 (3) the circumstances make it unjust for Microsoft to retain the benefit without payment. *See id.*

14 Cousineau's first unjust enrichment theory is that her purchase of a phone with a  
15 defective privacy control entitles her to the difference in price between a properly functioning  
16 phone and a dysfunctional phone. Cousineau has not pled facts sufficient to make this theory  
17 plausible. For example, Cousineau has not alleged any facts supporting the claim that the value  
18 of her phone actually diminished as a result of the defect in the privacy control on the camera  
19 application. Nor does she proffer a single price point or any other market data to support her  
20 theory. Without further facts, this allegation remains too speculative to support a plausible claim  
21 for relief.

22 Cousineau's second unjust enrichment theory is similarly unavailing. Cousineau asserts  
23 that Microsoft is not entitled to the economic benefit it derived from unlawfully collecting her  
24 data at the expense of her privacy. The problem with this theory, however, is that Cousineau  
25 focuses unduly on the benefit to Microsoft despite the fact that she must allege not only that  
26 Microsoft benefited but also that *she herself was deprived* in terms of payment, property,

1 services, or some equivalent form of an expense. *See Young*, 191 P.3d at 1264. Cousineau does  
2 not offer any facts supporting a reasonable inference that she suffered an economic loss on  
3 account of Microsoft’s purported appropriation of her data. Of course, Cousineau does argue that  
4 she suffered a non-economic loss—a loss of privacy—as a result of Microsoft’s conduct.  
5 However, to the Court’s knowledge, Washington courts have not applied the doctrine of unjust  
6 enrichment outside the context of an “expense” stemming from some tangible economic loss to a  
7 plaintiff. Plaintiff’s own authority is unhelpful in this respect. For example, in *Keithly v. Intelius*  
8 *Inc.*, plaintiffs alleged a clear economic expense. 764 F. Supp. 2d 1257, 1271 (W.D. Wash. 2011)  
9 *reconsidered on other grounds*, No. C09-1485-RSL, 2011 WL 2790471 (W.D. Wash. May 17,  
10 2011) (finding that plaintiffs had stated a claim for unjust enrichment where they alleged that  
11 defendant had deceived them into unknowingly purchasing online services that they did not  
12 want).

13         In light of the above, the Court finds that Cousineau has failed to state a plausible unjust  
14 enrichment claim.

15 //

16 //

17 //

18 //

19 //

20 //

21 //

22 //

23 //

24 //

25 //

26 //

1       **III. CONCLUSION**

2           For the foregoing reasons, Microsoft's motion to dismiss (Dkt. No. 22) is DENIED IN  
3 PART and GRANTED IN PART. The Court ORDERS that:

4           (1) Microsoft's motion to dismiss for lack of subject matter jurisdiction on the basis of  
5 standing is DENIED.

6           (2) Microsoft's motion to dismiss for failure to state a claim is DENIED with respect to  
7 Cousineau's claim under the Stored Communications Act.

8           (3) Microsoft's motion to dismiss for failure to state a claim is GRANTED with respect  
9 to Cousineau's Wiretap Act, Washington Consumer Protection Act, Washington  
10 Privacy Act, and unjust enrichment claims.

11          DATED this 22nd day of June 2012.

12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26



John C. Coughenour  
UNITED STATES DISTRICT JUDGE